Dicle University
Journal of Engineering
https://dergipark.org.tr/tr/pub/dumf
duje.dicle.edu.tr

Araştırma Makalesi/Research Article

Kişisel Siber Güvenlik Yaklaşımlarının Değerlendirilmesi

Evaluation of Personel Cyber Security Approaches

Muhammed Zekeriya GÜNDÜZ[1*], Resul DAŞ[2]

[1]Bingöl Üniversitesi, Bilgisayar Teknolojileri Bölümü, mzgunduz@bingol.edu.tr
ORCID: 0000-0003-4278-7123
[2]Fırat Üniversitesi, Yazılım Mühendisliği Bölümü, rdas@firat.edu.tr
ORCID: 0000-0002-6113-4649

MAKALE BİLGİLERİ

Makale Geçmişi:

Geliş 29 Mayıs 2022
Revizyon 22 Haziran 2022
Kabul 24 Haziran 2022
Online 30 Eylül 2022

Anahtar Kelimeler:

Siber güvenlik, Son kullanıcı, Parola güvenliği, Siber güvenlik farkındalığı, Mahremiyet

ÖZ

Bir birey hakkındaki herhangi bir veri, kişisel veri olarak kabul edilir. Bu kişisel veriler bireyi benzersiz bir şekilde tanımlayan değerlerdir. İsim, soy isim, kimlik numarası, anne kızlık soyadı ve benzeri şekillerde olabilen bu veriler bireyin kimliğini belirlemek için kullanılmaktadır. Ayrıca, bireyin çevrimiçi paylaştığı resimleri, mesajları, sağlık, eğitim, finans ve istihdam gibi verileri de kişiyi çevrimiçi olarak tanımlamada kullanılabilir. Bu sebeple kişisel düzeydeki verilerin ve bilgi işlem cihazlarının korunması gerekmektedir. Bu bağlamda; siber güvenlik, ilgili ağa bağlı sistemleri ve tüm verileri yetkisiz kullanımdan veya zarardan korumak için gereken çabaların bütünü olarak tanımlanır. Kişisel siber güvenlik ise bu çabaların bir kısmının siber farkındalık ile son kullanıcılar tarafından da gerçekleştirilmesidir. Son kullanıcıların sistem ya da veri güvenliğindeki en önemli görevlerinden birisi güvenli parola oluşturmalarıdır. Bu çalışma çevrimiçi bireysel kimlik verilerinin güvenliğinin sağlanması kapsamında güvenli parola oluşturulması için son kullanıcılara yönelik yeni yaklaşımlar önermektedir.

ARTICLE INFO

Article history:

Received 29 May 2022
Received in revised form 22 June 2022
Accepted 24 June 2022
Available online 30 September 2022

Keywords:

Cyber security, End user, Password security, Cyber security awareness, Privacy

ABSTRACT

A data about any person is considered personal data. These personal data are values that uniquely identify an individual. These data, which can be in the form of name, surname, identity number, mother's first surname and similar forms, are used to determine the identity of the individual. In addition, data such as pictures, messages, health, education, finance and employment that the individual shares online can be used to identify the person online. For this reason, it is necessary to protect the data and computing devices at the personal level. In this context; cyber-security is defined as all efforts to protect related networked systems and all data from unauthorized use or damage. Personal cyber-security, on the other hand, is the realization of some of these efforts by end-users with cyber awareness. One of the essential tasks of end-users in the system or data security is to create secure passwords. This study proposes new approaches for end-users to create secure passwords within the scope of ensuring the security of online individual identity data.

Doi: 10.24012/dumf.1122997

* Sorumlu Yazar

Giriş

İlk olarak 1948 yılında Norbert Wiener tarafından kullanılan siber [1] kavramı için farklı tanımlar bulunmaktadır. Bu tanımların hepsini kapsayacak şekilde siber kavramını; sayısal verinin olduğu her yer olarak tanımlamak mümkündür. Siber, sadece internet değildir. Siber kavramı, interneti de içerisinde barındıran daha kapsamlı bir terimdir. Hiç internet bağlantısı olmayan bir elektronik cihaz da siber ortamın bir parçasıdır. Dolayısıyla bu cihaza da atak yapılabilir, verileri çalınabilir ve değiştirilebilir. Ayrıca, internete bağlı ağ sistemleri olduğu gibi, bağlı olmayanlar da olabilir. İnternete bağlı olmadığı halde önemli kararların bilgisayarlar tarafından alındığı demiryolu ağı, metro ağı, otomasyon ağları gibi sistemlerde bulunan cihazlar da siber ortamın içerisinde bulunurlar. Bu sistemler, güvenlik gereksinimleri nedeniyle özellikle internet ağına bağlanmazlar. Ancak nesnelerin interneti kavramı bu sistemlerin de internet ağına bağlanmasının zaruretini ortaya çıkarmaktadır [2].

Günümüzde, siber ortamda bulunan veri, cihaz ve sistemlerin güvenliğinin sağlanması için siber güvenlik yaklaşımlarının sayısal tüm ortamlarda vazgeçilmez bir sistem bileşeni olduğu görülmektedir [3]. Güvenlik ortada kıymetli bir meta bulunduğunda gereklidir. Bu meta bir veri, veritabanı, donanım elemanı ya da sistemin tamamı olabilir. Dolayısıyla siber ortamda bulunan verinin güvenliğinin sağlanması bir zorunluluktur. Bu bağlamda, siber güvenlik dendiğinde genelde siber ortamda bulunan verinin güvenliğinin sağlanması anlaşılır. Bir şirketin satış detaylarını içeren verileri, bankanın müşteri bilgileri gibi veriler kıymetlidir. Kıymetli bir metanın olduğu yerde onu gayri meşru şekilde ele geçirmek isteyenler olabilir. İnsanoğlunun bu gayri meşru eylemlerinin olmadığı kabul edilse idi, siber güvenlik kavramının ortaya çıkmasına gerek kalmayacaktı. Böyle bir durum söz konusu olmadığı için siber güvenlik kavramı sayısallaşan dünyada daha fazla önem kazanmaktadır.

Sayısal ortamdaki veriler içeriklerine göre çeşitlilik gösterirler. Tıbbi kayıtlar (reçeteler, elektronik sağlık kayıtları vs.), tüketim bilgileri (mağaza sadakat kartları, alışveriş sitelerindeki kişisel veriler vs.), eğitim kayıtları (notlar, sınav puanları, alınan dersler, ödüller, dereceler, devamlılık, disiplin raporları), sosyal medya hesaplarındaki bilgiler, istihdam ve finansal kayıtlar (gelir-giderler, vergi kayıtları, bankacılık ekstreleri, kredi notu, geçmiş istihdam ve performans), arama motorlarında yapılan arama kayıtları, mobil cihazlarda tarayıcı tarafından kaydedilen kullanıcı adı ve parola verileri bunlardan bazılarıdır [4]. Bu kişisel verilerin özellikle sosyal mühendislik [5] gibi insan zafiyetinin sömürülmesine yönelik olan saldırılara karşı korunması için etkin yöntemler geliştirilmelidir.

Son kullanıcıların kişisel veri güvenliği açısından yerine getirmeleri gereken en önemli görevlerden birisi güvenli parola oluşturabilme yeteneğine sahip olabilmeleridir. Ayrıca, "şifre" ve "parola" ifadelerinin farklı kavramlar olduğunun farkına varılması son kullanıcı tarafından bilinmelidir. Dolayısıyla kavramların Türkçe karşılığının doğru kullanımının sağlanması açısından şifre kelimesi değilde parola kelimesi çalışma boyunca kullanılmıştır. Şifre ifadesi kriptoloji bilimi içerisinde kullanılan ve düz metin bir ifadenin şifreli metin haline getirilmesi sürecinde kullanılan bir terim iken, parola ifadesi ise bir sisteme dahil olabilmek için kullanılan bir karakter kümesini ifade etmektedir.

Son kullanıcıların etkili ve güvenilir parolalar oluşturması açısından farklı güncel çalışmaların yapıldığı görülmektedir. [6] numaralı çalışmada; dijital bir sistemde en zayıf halkanın insan olduğu belirtilmiş ve bu durum birçok kullanıcının oluşturduğu zayıf parolaların çok kısa sürelerde kırılması ile ortaya konmuş ancak güçlü parola oluşturma açısından güncel bir yaklaşım önerilmemiştir. [7] numaralı çalışmada; insanoğlunun dijital ortamda parolalar oluşturmaya başladığı yaklaşık yarım asırlık süreçte güçlü parolalar oluşturma yeteneğini kazanmadığı ortaya konmuş olup, hatırlanması kolay parola oluşturma yöntemlerinden kısaca bahsedilmiştir. [8] numaralı çalışmada; son kullanıcıların daha hatırlanabilir ve güvenli parola oluşturması açısından farklı güncel yöntemler önerilmiş olup bu yöntemlerin adım sayısının genellikle üçden fazla olması uygulanabilirlik açısından zorluk teşkil etmektedir. [9] numaralı çalışmada; son kullanıcıların göz hareketlerini izleyerek yapay zeka temelli bir parola üreteci oluşturulmuş olup oluşturulan parolanın kullanıcı için anlamlı ve hatırlanabilir olması konusunda bir öneride bulunulmamıştır. Konu ile ilgili literatür detaylı incelendiğinde güçlü parola oluşturmaya yönelik yeni yaklaşımlar göze çarpmaktadır. Ancak oluşturulan güçlü parolaların son kullanıcılar tarafından kolaylıkla hatırlanmasını sağlayacak farklı yöntemlerin azlığı dikkat çekmektedir. Bu bağlamda son kullanıcıların, bilindik klasik yöntemlerden farklı olarak etkin, güncel, güvenli ve hatırlanabilir parola oluşturma teknikleri ile alakalı Türkçe akademik yayına rastlanmamış olması bu çalışmanın ortaya çıkmasına temel oluşturmuştur. Genellikle sistem yöneticileri tarafından kullanılan parola oluşturma yöntemlerinin son kullanıcıya uyarlanabilecek bazı tarzları çalışmada sunulmuştur. Bu bağlamda çalışma, siber güvenliğin son kullanıcılara yansıması açısından farklılığını ortaya koymaktadır. Ayrıca çalışmada; siber ortamdaki çevrimiçi kişisel verilerin korunması için yapılacakların belirlenmesi, kişisel verilerin korunmasına yönelik geleneksel ve güncel yaklaşımların değerlendirilmesi amaçlanmıştır.

Çalışmanın ikinci bölümünde siber ortamda kişisel veri güvenliğine zarar veren bileşenler ele alınmaktadır. Üçüncü bölümde bu zafiyetlere karşı varlıkların korunması için gerekli önlemler değerlendirilmektedir. Dördüncü bölümde ise varlıkların korunmasına yönelik etkin parola oluşturma yaklaşımları önerilmektedir. Son bölümde çalışma güncel yaklaşımlar ışığında değerlendirilmektedir.

Kişisel veri ve siber güvenlik zafiyetleri

Siber ortamda bulunan bir veri veya sistem; gizlilik, bütünlük ve erişilebilirlik ilkelerini sağlıyor ise güvenli kabul edilir [10]. Gizlilik, verinin yetkisi olmayan başka bir kişi tarafından görülmemesi/okunmamasıdır. Bütünlük, verinin orijinal halinin her durumda sağlanması ve yetkisiz üçüncü taraflarca değiştirilememesidir. Erişilebilirlik, veriye erişim yetkisi olan taraflarca belirlenmiş zamanlarda erişilebilmesidir. Bu üç ilkeden herhangi birinin sağlanamaması güvenlik zafiyeti olarak adlandırılır.

Kişisel veri

En genel tanımıyla kişisel veri, belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgidir [11]. O halde kişisel veriden söz edebilmek için, verinin (i) bir kişiye ilişkin ve (ii) bu kişinin de belirli ya da belirlenebilir nitelikte olması gerekir. Bu tanımda "her türlü" bilgi ifadesinin kullanılması oldukça geniş bir alanın hedeflendiğinin işaretidir. Burada bilginin türüne ilişkin herhangi bir ayrım yapılmamaktadır. Sayı, yazı, ses ya da görüntüden oluşan bir bilgi bu kapsamda yer alabilir.

Kişiyi doğrudan ya da dolaylı olarak belirlenebilir kılan kişisel veriler; bir kişinin adı, soyadı, adresi, telefon numarası, pasaport numarası, resmi, ses kaydı, genetik bilgileri, cinsel tercihleri, dini inançları, sabıka kaydı, hobileri, ziyaret ettiği internet siteleri gibi bilgiler bu kapsamda değerlendirilir. Siber bağlamda ise kişiye ait her türlü sayısal değer kişisel veri olarak nitelenir. Kişisel veriler, bireyin kişisel kimlik bilgilerini de içerir. Kimlik bilgileri ile kastedilen kişiyi tanımlayabilecek her türlü veridir. Kişisel veriler, dijitalleşmenin artması ile siber ortamlarda daha fazla bulunur hale gelmiştir [12]. Resim, dosya, parola gibi sayısal veriler hem taşınabilir bellek, sabit disk, optik disk, hafıza kartı gibi kişisel cihazlarda hem de web sitesi, bulut gibi harici çevrimiçi ortamlarda da depolanabilir. Dolayısıyla bu kapsamdaki bilgiler, kişisel verilerin korunmasında hâkim olan temel ilkelere göre işlenmeli ve depolanmalıdır.

Bireylerin çevrimiçi ve çevrimdışı kimliği bulunur. Çevrimiçi kimlik, siber alandaki kimliği ifade ederken, çevrimdışı kimlik ev, okul, iş gibi sosyal ortamlarda kişiyi niteleyen ve etkileşim kurmasını sağlayan kimliğidir. Bu çalışmada çevrimiçi kimlik verilerini koruma yolları değerlendirilmektedir. Devletler tarafından bu verileri koruma altına almak için çeşitli kanunlar yürürlükte olsa da, asıl olan son kullanıcıların siber güvenlik farkındalıklarının yüksek olmasının sağlanmasıdır. Ülkemizde 2016 yılında yürürlüğe giren KVKK (Kişisel Verileri Koruma Kanunu), kişisel verileri bulunduran kurumların bu verileri nasıl koruyacaklarının belirlenmesi açısından önemlidir.

Çevrimiçi kimlik siber uzayda kişiyi başkalarına tanımlar. Bu çevrimiçi kimlik, son kullanıcı ile ilgili sınırlı miktarda bilgiyi içermelidir. Dolayısıyla; çevrimiçi kimlik için kullanıcı adı veya takma ad seçilirken herhangi bir kişisel bilgi içermemesi konusunda dikkatli olunmalıdır. Bu kullanıcı adı, siber saldırganlar için son kullanıcının kolay bir hedef olamayacağını göstermelidir [13].

Siber saldırganlar

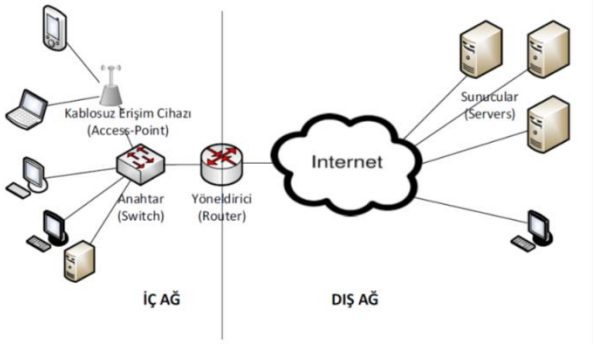
Siber ortamda gerçekleştirilen bir saldırının sorumlularını net bir şekilde bulmak kolay değildir. Bu saldırgan(lar) her cinsten, ırktan, yaştan, gruptan olabilir. Bu saldırı bir yapay zekâ ürünü bile olabilir. Saldırı sonucu kişisel verileri elde eden saldırganlar; kurban adına kredi kartı hesabı açma veya kredi alma, hedef bilgisayarı ele geçirme, kayıtlı parolaları elde etme, dosyaları silme, değiştirme, şifreleme gibi işlemler yapabilirler.

Siber saldırganlar, kişisel veya finansal kazançlar için güvenlik açığından yararlanmaya çalışan kişiler veya gruplardır. Amatör olarak siber atak gerçekleştirmeye çalışan saldırganlar, teknik bilgileri olmayıp hazır araçlar ile ufak saldırılar gerçekleştirmeye çalışırlar ve genellikle iz bıraktıkları için tespitleri çok kolaydır. Kişisel verilere yönelik saldırılarda amatör saldırganlar önemli bir paya sahiptirler. Profesyonel saldırganlar ise beyaz şapkalı (ethical hacker), siyah şapkalı ve gri şapkalı olarak üç sınıfa ayrılırlar. Siyah şapkalı saldırganlar, siber güvenliğe zarar verecek faaliyetleri, para kazanma, kişisel tatmin, politik sebepler gibi nedenlerden dolayı yasadışı gerçekleştirirler. Beyaz şapkalılar ise yasal bir şekilde bir sistemin zafiyetlerini tespit edip gerekli önlemleri almayı amaçlarlar. Sızma testleri beyaz şapkalılar tarafından yapılır. Gri şapkalılar beyaz ve siyah şapkalılar arasında yer alırlar. Belirledikleri bir sisteme sızarak, zafiyetleri tespit edip bunu para karşılığında saldırdıkları kişi/kurum veya üçüncü şahıslara bildirirler/satarlar. Bir sistemin açığını illegal olarak bulmak yasal suçtur. Dolayısıyla gri şapkalılar da siyah şapkalılar gibi yasadışı kabul edilirler. Bu saldırganlar bireysel olabileceği gibi genelde ekip halinde çalışırlar, organizedirler ve para elde etmeyi amaçlarlar [14].

Siber saldırı süreci

Son kullanıcıların bir ağ sistemini detaylı bilmeleri beklenemez. Ancak temel seviyede bir ağ yapısını bilmek saldırıların sürecini anlamayı kolaylaştırır. Bu durum son kullanıcıya kişisel siber güvenlik açısından farkındalık kazandırır. Şekil-1 de görüldüğü gibi yönlendirici cihazın internete bağlı kısmı dış ağı, diğer kısmı ise iç ağı oluşturur. Son kullanıcıyı daha fazla ilgilendiren kısım iç ağdır. İç ağ; ev, ofis, laboratuvar, bina vb. küçük ölçekli bir yerel ağdır. İç ağlarda özellikle kablosuz erişim cihazlarından veri dinlenmesi kablolu erişimde kullanılan anahtar cihazlara göre nisbeten daha kolaydır. Dış ağ seviyesindeki veri güvenliği son kullanıcının kontrolü dışındadır. Hem iç hem dış ağ yapısının temel olarak bilinmesi son kullanıcının bilgi güvenliği farkındalığı için önemlidir.

Bir siber saldırı sırası ile; keşif atakları, erişim atakları, servis dışı bırakma atakları olmak üzere üç aşamalı olarak gerçekleştirilir. Keşif atakları ile sistemdeki güvenlik zafiyetlerinin tespit edilmesi amaçlanır. Keşif atakları hedefin kişi veya kurum olmasına göre değişkenlik gösterir. Erişim atakları ile bulunan açıklar kullanılarak hedef sisteme sızma gerçekleştirilmeye çalışılır. Eğer saldırganlar sisteme erişim sağlayamaz ise sistemi servis dışı bırakma atakları ile erişilemez hale getirmeyi amaçlar [15].



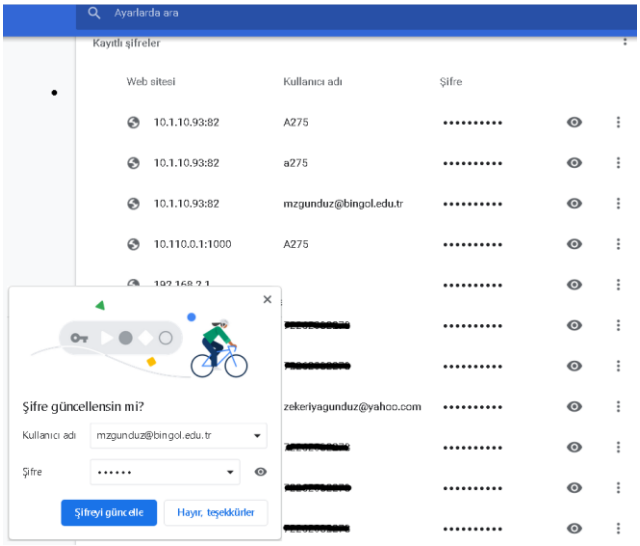
Şekil 1. Tipik bir ağ mimarisi.

Keşif atakları hedef ile ilgili internetten bilgi araştırması, ping taraması, port taraması, paketlerin dinlenmesi işlemlerini içerir. Örneğin hedef cihazın Ip adresi ping atılmak sureti ile elde edilebilir. Elde edilen Ip adresi sayesinde, ripe.net gibi veri tabanlarından whois sorguları yapılarak hedef hakkında kullandığı gerçek ip adres aralığı, bağlı olduğu ağ adı, bulunduğu ülke gibi temel seviyede bilgiler elde edilebilir. Özellikle elde edilen gerçek Ip adres aralığı, bu ağda dışardan erişilebilecek sunucu, yönlendirici, anahtar, bilgisayar cihazlarının varlığı hakkında bilgi verir. Bu Ip adres aralığındaki değerler aynı şekilde sorgulanarak temel bilgiler elde edilebilir. Elde edilen Ip adres aralığından angry ip scanner, nmap gibi bir yazılım ile bu aralıktaki tüm aktif cihazların adı, açık portları, MAC adresi, Ip adresi gibi bilgiler elde edilebilir. Erişilen ağdaki paketlerin içeriği ise wireshark gibi bir yazılım aracılığı ile incelenebilir [16].

Keşif aşamasında hedefin kişi veya kurum olmasına göre keşfedilmesi gereken parametreler ve kullanılacak ataklar değişir. Hedef; kişi ise keylogger, phishing mails, warez siteler (bedava yazılım, crack'li oyun/program veren siteler) vs. gibi kısa sürede sonuç verecek yöntemler kullanılır. Hedef bir kurum ise saldırı süreci, daha uzun süre ve organize bir yapı gerektirir. İnternet bilgi araştırması (Ip adresi, e-posta, sosyal medya araştırmaları vs.), ping taraması, port taraması, paketleri dinleme işlemleri yapılır. Bilgisayar ve sunucuların açıklarını tespit etmek için farklı tarama araçları kullanılır. Bu sayede sistem ile ilgili zafiyetler elde edilir [16].

Keşif aşamasında elde edilen bu bilgilerden sonra erişim aşamasına geçilir. Bu aşamada gizlilik-bütünlük-erişilebilirlik ilkelerinden hangisine yönelik saldırı hedefleniyorsa saldırı süreci ona göre şekillenir. Bu doğrultuda, parolaların ele geçirilmesi, yazılımsal hatalardan (bug) yararlanılması (işletim sisteminde buffer overflow, web sayfalarında sql injection, xss vb.), ortadaki adam ataklarının gerçeklenmesi, zararlı yazılımların (virüs, solucan, Truva atı vb.) koşturulması gibi işlemler ile sisteme yetkisiz erişim sağlanmaya çalışılır.

Sunucu veya kişisel cihazların geçerli parolalarını ele geçirmek için en çok kullanılan yöntem kaba kuvvet saldırısıdır. Bu yüzden parolalar basit olmamalıdır [17]. Parola saldırıları, kişilerden ziyade zararlı yazılım bulaşmış cihazlar tarafından gerçekleştirilir. Bir web tarayıcısının kaydettiği tüm parolalar, bilgisayarın genel parolasını ele geçiren biri veya zararlı üçüncü parti yazılımlar tarafından kolaylıkla ele geçirilebilir. Bir saldırgan sadece kişinin bilgisayar parolasını ele geçirerek, Şekil 2'de görüldüğü gibi diğer tüm parolaları da ele geçirebilir. Bu parolalar makine ele geçirildiğinde çalınabilir, dolayısıyla tarayıcıya parola kaydetmek güvenlik riski oluşturabilir. Özellikle ssh portu açık olan sunucu, router gibi cihazlara erişmek için yapılan kaba kuvvet saldırıları günümüzde hala en etkili saldırıdır.



Şekil 2. Tarayıcı tarafından parola kaydedilmesi.

Https protokolü verinin şifreli gitmesini sağlar. Https protokolünün kullanılmadığı ağlarda ortadaki adam saldırısı ile kullanıcının tüm trafiğinin saldırgan cihazdan geçmesi sağlanabilir. Sahte DHCP, DNS, web sunucuları üretilerek bu işlemler gerçekleştirilebilir. Bu konular daha çok ağ güvenliği konusunda değerlendirilmektedir. Bu çalışma kapsamında son kullanıcıya ait verilerin güvenliğinin sağlanması ele alındığından detaya girilmemiştir.

Siber varlıkların korunması

İkinci bölümde bir siber saldırının nasıl gerçekleştirildiği ve saldırganların bir sistemi ele geçirmek için hangi yöntemleri kullandıkları üzerinde

duruldu. Bu bölümde ise ikinci bölümde bahsedilen siber saldırılara karşı siber varlıkları savunmak için kişisel düzeyde sağlanması gereken temel çözümlerden bahsedilmektedir.

Son kullanıcının verilerine erişmek için virüs, truva atı, solucan, fidye yazılımı, casus yazılım gibi zararlı yazılımlar son kullanıcının izni veya haberi olmadan bilgisayar, mobil/akıllı cihazlarına bulaşabilir. Verinin depolanmasını ve üzerinde işlem yapılmasını sağlayan bu cihazlar siber ortamın kapısıdır. Bu bağlamda, siber ortama bağlanacak son kullanıcı cihazlarının siber saldırılara karşı temel güvenliğinin sağlanması için bir takım önlemler son kullanıcı tarafından alınmalıdır.

İşletim sistemi güncellemelerinin yapılması: Her yazılım bir zafiyet veya yazılımsal hata barındırabilir. Dolayısıyla, ağ cihazları, bilgisayar, cep telefonu gibi İnternete bağlanan cihazların işletim sistemi güncellemeleri düzenli olarak yapılmalıdır. Güncellemeler işletim sistemine yeni özelliklerin eklenmesi, mevcut olanların iyileştirilmesi ve güvenlik zafiyetlerinin giderilmesini sağlarlar. Ağ cihazlarının da güvenlik açıkları olabilir, dolayısıyla güncellenmeleri gerekir. ADSL modem gibi ağ cihazlarının güncellemeleri orijinal kaynaklarından indirilecek firmware yazılımları ile sağlanmalıdır. Yazılım güncellemelerinin amacı sistemin güncel kalması ve güvenlik zafiyetlerini düzeltmektir.

Lisanslı yazılım kullanılması: Lisanslı yazılım kullanılması, ilgili yazılım fonksiyonlarının tam ve eksiksiz çalışmasını sağlar. Virüs riskine karşı güvenlidir. Orijinal yazılım kullanmak yasal yaptırımlara maruz kalınmasını engeller. Ayrıca orijinal olmayan yazılımlarda siber güvenlik açısından güvenilir bir güncelleme yapılamaz.

Kaynağı bilinmeyen yazılımların kullanılmaması: İnternet ortamı, taşınabilir bellek, e-posta aracılığı ile elde edilen, içeriği ve kaynağı tam olarak bilinmeyen özellikle exe, inf, bat, com uzantılı dosyalar kesinlikle çalıştırılmamalıdır.

Crack yazılım kullanımında dikkatli olunması: Oyun, resim, video gibi programlar genelde paralıdır. Bu programlar genelde ücretsiz olarak elde edilmek istendiği için crack halleri kullanılır. Crackli bir yazılımın muhtevası tam olarak bilinemediğinden ciddi güvenlik risk içerir. Çünkü çıkar sağlamaksızın ücretli bir oyun ücretsiz bir şekilde dağıtılmaz. Crackli yazılım barındıran cihazların güvenilirliği şüphelidir. Crack yazılım kullanmak konusunda ısrar edilirse sanal makine üzerine kurulacak bir işletim sisteminde çalıştırılması güvenlik riskini minimize eder. Crackli yazılım bulunan cihazda önemli işlemler yapılmamalıdır. Bir programın crack hali tersine mühendislik ile elde edilir.

Güvenli bağlantıya dikkat edilmesi (Https): Kullanıcı adı, parola verilerinin girildiği bir web sitesinin https protokolü kullanması gerekir. Https, bilgilerin şifreli bir şekilde gitmesini sağlar. Sayfanın herhangi bir köşesinde kilit işareti çıkmalıdır. Özellikle çevrimiçi bankacılık sitelerinde sitenin adı yeşil ile yazılır. Ayrıca kullanıcı adı ve parola girilecek siteler bir link aracılığı ile değil de bizzat yeni bir sahifede açılmalıdır.

Güvenlik Duvarının aktif edilmesi: Saldırganların kişisel veya kurumsal verilere erişmesini önlemek için bilgisayar güvenlik duvarı aktif ve güncel olmalıdır. Güvenlik duvarı, talep edilmeyen trafiği engelleyen yazılımdır. Birçok işletim sisteminde güvenlik duvarı varsayılan olarak açık gelir. Bazı programların yüklenmesi, bir ağa bağlanılması gibi durumlarda güvenlik duvarının kapatılması gerekebilir. İlgili işlem bittikten sonra tekrar açılmalıdır. Özellikle kamuya açık bir kablosuz ağda kesinlikle açık olmalıdır [18]. Güvenlik duvarı filtreleme yapar, ağın içine yetkisiz erişimi engeller. Bu, son cihaza yetkisiz erişimi engelleyen host-based bir güvenlik duvarı sistemini veya dış ortamdan ağa yetkisiz erişimi önlemek için ana yönlendiricide (home router) temel bir filtreleme hizmetini içerebilir.

Antivirüs yazılımı kullanımı: *S*on cihazlara kötü amaçlı yazılım bulaşmasına karşı koruma sağlar. Son kullanıcı cihazında yüklü olan antivirüs yazılımı, en yeni kötü amaçlı yazılımlardan korunmak için güncel tutulmalıdır. Özellikle internet ortamında sörf yapmak, crackli program kullanmak gibi kullanım alışkanlığına sahip kullanıcılar anitivirüs yazılımı kullanmalıdır. Antivirüs, cihazın performansını belli oranda düşürebilir. Dolayısıyla, antivirüs yazılımı kullanmak istemeyen kullanıcılar girdikleri bir sitenin veya indirdikleri bir dosyanın güvenliğini denetlemek için Cisco firmasına ait olan ve birçok antivirüs firmasının veritabanını tarayan, referansta verilen, ücretsiz çevrimiçi uygulamayı kullanabilir [19]. Ayrıca, hiçbir antivirüs yazılımının %100 güvenlik sağlayamayacağı unutulmamalıdır.

E-postalardaki linklere tıklanmaması: Bir e-postanın kimden geldiğine, gidilen linke dikkat edilmelidir. Bilinmedik bir e-postadan gelen linke veri girilmemelidir. Bunlar genelde spam klasörüne düşer. Şüpheli bir e-postada verilen link, arama motorunda aranmalıdır, linkin ne hakkında olduğu forumlardaki yorumlardan anlaşılacaktır. Dolayısıyla kesinlikle verilen linke tıklanıp yönlendirilen sitede kullanıcı adı / parola girilmemelidir. Ayrıca eklerde gelen exe, zip uzantılı dosyalar çok daha dikkatli açılmalıdır. Kullanıcı ile alakalı olmayan veya beklenen kişiler tarafından gönderilmemiş e-posta mesajlarının açılmamasına dikkat etmek çok önemlidir. E-posta açılmadan önce konu alanı ve gönderen adresi kontrol edilmelidir.

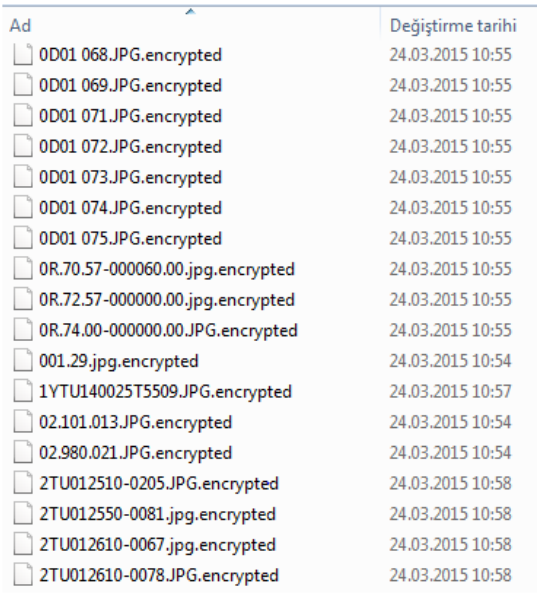
Çevrimiçi ortamlarda kişisel veri mahremiyetinin sağlanması: Bilgisayar, cep telefonu ve mobil cihazlar birer kişisel veri deposu halini almıştır. Ayrıca, sosyal

medya platformlarının ortaya çıktığı ilk yıllarda son kullanıcılar kişisel bilgilerini kontrolsüz bir şekilde paylaştılar. Bu durum birçok mağduriyetlere sebep olmaya devam etmektedir. Bu bağlamda; veri mahremiyetini sağlamak için son kullanıcılar tarafından sosyal medya ortamlarında gereksiz bilgi paylaşımı yapılmamalıdır. Sosyal medya profilleri gerekli en az kişisel veri ile doldurulmalıdır. Aşırı miktarda çevrimiçi kişisel bilgi paylaşımı, kötü niyetli kişilerce o kişi adına bir profil oluşturulmasını kolaylaştırır. Anne kızlık soyadı, doğum tarihi, doğum yeri gibi kritik olabilecek veriler tam olarak verilmemelidir. Sosyal medya ayarları sadece istenen kişilerin katılabileceği, görebileceği, yorum yapabileceği şekilde ayarlanmalıdır.

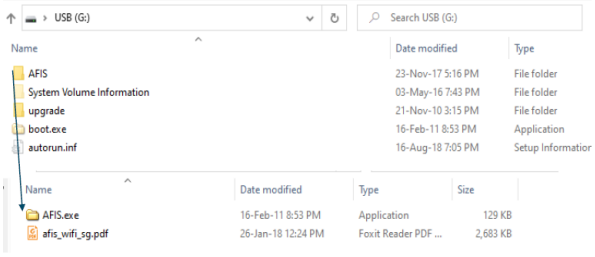
Tarayıcı gizlilik ayarlarının doğru yapılması: Son kullanıcının bilgisayarına veya ev yönlendiricisine erişimi olan bir saldırgan, bu kişinin web tarayıcı geçmişine, önbellek, kayıt(log) dosya verilerine erişerek kullanıcının profili hakkında bilgileri ele geçirebilir. Bu sorun web tarayıcısının sahip olduğu özel korumalı mod sayesinde en aza indirgenebilir. Örnek olarak Google Chrome web tarayıcısının özel korumalı modu *gizli pencere*dir. Özel korumalı mod kullanıldığında çerezler devre dışı bırakılır, ayrıca geçici internet dosyaları ve tarama geçmişi tarayıcı kapatıldıktan sonra otomatik olarak silinir. İnternet tarama geçmişini gizli tutmak, kullanıcının çevrimiçi etkinlikleri hakkında bilgi toplanmasını ve hedefli reklamlara maruz kalınmasını engellemede oldukça etkilidir.

Düzenli yedek alınması: Verilerin yedekleri harici bir sabit diskte veya bulut ortamında tutulabilir. Fiziksel olarak ayrı bir depolama cihazında saklanacak ise bu cihaz ayrı bir yerde muhafaza edilmeli, her cihaza takılmamalı, sürekli bir şekilde bilgisayara takılı tutulmamalıdır. Bulut da yedek alınacak ise yedekleme anında bağlantı kurulur, yedekleme bittikten sonra bağlantı kapatılır. Eğer bulut ortamı devamlı açık tutulur ise crypolocker gibi saldırılar şekil-3 deki gibi buluttaki verileri de şifreleyebilir. Bulutun asıl amacının yedeklemekten ziyade farklı cihazlardan senkron çalışmaya olanak sağlamak olduğu da unutulmamalıdır. Bulut ortamındaki dosyalara bulaşmış bir zararlı yazılım var ise dosyaların silinmesinden başka bir yol yoktur.

Taşınabilir belleklerin dikkatli kullanılması: Taşınabilir bellekler virüs, truva atı, casus yazılım, solucan gibi birçok zararlı yazılımın yayılması için elverişli cihazlardır. Özellikle Windows işletim sistemleri için "Gizli dosyaları, klasör ve sürücüleri göster" seçeneği exe, inf, com, bat uzantılı dosyaları görmek için aktif olmalıdır. Çünkü bu dosyalar gizli dosyalardır. Bununla birlikte "Bilinen dosya türleri için uzantıları gizle" ve "Korunan işletim sistemi dosyalarını gizle" seçili olmamalıdır. Bu ayarların belirtildiği gibi olması durumunda virüslü bir taşınabilir belleğin içeriğinin nasıl görüleceği şekil-4 de gösterilmiştir.

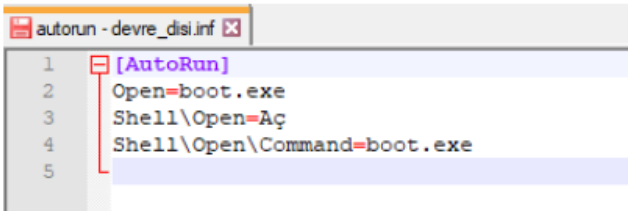


Şekil 3. Cryptolocker ile şifrelenmiş dosyalar.



Şekil 4. Virüslü dosya.

Autorun.inf dosyası varsayılan değerde son kullanıcıya kullanım kolaylığı sağlaması açısından Windows geliştiricilerince oluşturulmuş bir gizli dosyadır. CD, taşınabilir bellek gibi bir cihazın otomatik çalışmasını sağlar. Yani exe dosyasının otomatik çalışmasını sağlamak için kullanılır. Ancak bu faydalı özellik saldırganlar tarafından bir güvenlik zafiyeti olarak kullanılmaktadır ve virüs bulaşmış bir taşınabilir belleğin bilgisayara takıldığı anda otomatik olarak içindeki virüsü (boot.exe) çalıştırması için kullanılmaktadır. Bu dosyanın içerisindeki kod şekil-5 deki gibi virüs dosyası olan "boot.exe" dosyasını çalıştıracak şekilde ayarlanmıştır. Dolayısıyla autorun.inf dosyasının otomatik çalışmaması için "Otomatik kullan" özelliği devre dışı bırakılmalıdır."



Şekil 5. Örnek bir autorun.inf dosyasının içeriği.

Farklı parolaların kullanılması ve parolaların yönetimi: Son kullanıcıların birçok çevrimiçi hesabı olabilir. Her bir çevrimiçi hesap için farklı ve benzersiz parolalar kullanılmalıdır. Bu durum hatırlanması gereken birçok parola demektir. Güçlü ve benzersiz parolalar kullanmamak, son kullanıcı verilerini siber suçlulara karşı savunmasız kılabilir. Tüm çevrimiçi hesaplar için aynı parolayı kullanmak, sahip olunan tüm kilitli kapılar için aynı anahtarı kullanmaya benzer. Eğer bir saldırgan bu anahtarı ele geçirecek olursa, sahip olunan her şeye erişebilecektir. Bir saldırgan kimlik avı yoluyla bir parolayı ele geçirirse ve son kullanıcı tüm hesapları için aynı parolayı kullanıyorsa diğer hesaplarını da kolaylıkla ele geçirecektir.

Günümüz son kullanıcıları, hatırlanamayacak kadar parola gerektiren çevrimiçi hesap kullanmaktadır. Bir parola yönetici yazılımı kullanmak farklı, güçlü parolalar oluşturmak ve bunları şifreli olarak saklamak için bir çözüm olabilir. Bu yazılım, çevrimiçi hesaplarda otomatik olarak oturum açmada kolaylık sağlayacaktır. Bunun için, parola yönetici yazılımının parolasını bilmek yeterli olacaktır.

Tablo-1'de gösterilen ve en çok kullanılan parolalar kullanılmamalıdır. Kaba kuvvet saldırılarına karşı parolalar altı ayda bir yenilenmelidir. Ayrıca, parolaların sanal klavye ile girilmesi kısmi olarak tuş kaydedici yazılımlarına karşı güvenlik sağlar. Bu konu bölüm 4 de yeni yaklaşımlar ışığında detaylı olarak incelenmiştir

Tablo 1. En Çok Kullanılan Parolalar.

Dragon	12345678	654321	admin
1234	123456789	password	qwerty
12345	1234567890	password1	qwerty123
123456	123123	abc123	Princess
1234567	111111	Monkey	Iloveyou

Bu önlemlere ilave olarak; gönderilen e-postaların üçüncü kişiler tarafından okunmasını engellemek için gerekli protokoller aktif edilmelidir. Ayrıca, bilgisayar veya mobil cihazdan silinen hassas veriler, bu cihazlar teknik servise verme, satma vb. gibi üçüncü kişilerin eline geçtiğinde bile, ele geçirilemeyecek şekilde özel programlar ile kalıcı olarak silinmelidir. Bankacılık işlemlerini GSM teknolojilerinin sağladığı web hizmetleri üzerinden yapmak daha güvenilirdir. Özellikle Android işletim sistemine sahip kullanıcılar yükledikleri yazılımların güvenilirliği konusunda dikkatli olmalıdırlar.

Önerilen yeni yaklaşımlar

Önceki bölümlerde siber güvenliğin özellikleri ve karakteristiğinin yanında, çevrimiçi kimlik ve dijital verilerin siber saldırganlar açısından önemi son kullanıcı seviyesinde açıklanmıştır. Bu bölümde kişisel çevrimiçi kimlik ve verilerin siber güvenliğinin sağlanması parola yönetimi açısından yeni yaklaşımlar ile ele alınmaktadır.

Parola diş fırçası gibidir. Başkasının kullanmasına izin verilmez ve altı ayda bir değiştirilmelidir. Siber saldırganlar, aynı parolayı faklı web sitelerinde ve hesaplarda kullanmalarından dolayı, birçok son kullanıcının çevrimiçi kimlik ve hesap bilgilerini ele geçirebilirler. Tek parola ile aynı anda birden fazla işi yapmak (PC, mail, sunucu, VPN erişim parolaları gibi) tek parola ile her şeye girmek (single-sign-on) anlamına gelir ve bu güvenlik açısından sıkıntılı bir yaklaşımdır. Çünkü parolayı kaybetmek her şeyi kaybetmek anlamına gelir. Farklı parola algoritmaları geliştirmek bunun en uygun çözümüdür [13].

Muhtemel bir saldırıda, on karakterli bir parolada büyük harf, küçük harf, rakam ve özel karakterlerden oluşan bir parolanın kaba kuvvet saldırıları tarafından kırılması çok daha uzun olacaktır. Bir parolanın en az sekiz karakter içermesi önemlidir. İçerisinde sayısal olmayan bir karakter barındırması parolanın kırılma süresini yüzlerce yıla kadar çıkarmaktadır.

Güvenli parola oluşturmada temel adımlar

Parola isteyen uygulamalar tarafından güvenli parola oluşturma konusunda son kullanıcılara temel düzeyde bazı zorunlu yönlendirmeler yapılmaktadır. Bu yönlendirmeler genel olarak şu şekilde özetlenebilir:

- Sekiz veya daha fazla karakterden oluşan bir parola kullanılmalıdır.
- Herhangi bir dilde yaygın kullanılan kelimeler ve isimler kullanılmamalıdır.
- Özel karakterler (! @ # $ % ^ & * ( ) vb.) kullanılmalıdır.
- abc123 gibi kolay tahmin edilebilen parolalar kullanılmamalıdır.
- Ardışık rakam ve harfler tercih edilmemelidir.
- Parola ile ilgili ipucu soruları oluşturulmamalıdır.
- Küçük ve büyük harfler bir arada kullanılmalıdır.
- Bir dilin sözlüğünde bulunan kelimeler parola olarak kullanılmamalıdır.

Bu yönlendirmeler kullanıcının iyi bir parola oluşturması için yeterli olur. Ancak daha güçlü parolaların oluşturulması ve bunların hatırlanması son kullanıcılar için zor olabilmektedir. Tablo-2 de Normal-İyi-En İyi olarak oluşturulan parola örnekleri gösterilmiştir. Oluşturulan parolalar belli bir algoritmaya veya yapıya göre oluşturulmaz ise son kullanıcılar için kontrolü zor durumların ortaya çıkmasına sebep olabilmektedir. Günümüzde parola kullanımı e-devlet, eğitim, sağlık, banka işlemleri gibi birçok web uygulamasında kullanılmaktadır. Bu kadar çok parolanın yönetimi için kağıda yazmak, aynı

parolayı her yerde kullanmak, parola yönetim uygulamaları kullanmak gibi çeşitli yöntemler geliştirilmiştir. Ancak bu yöntemlerin de güvenlik zafiyetleri içerdiği bilinmektedir. Güçlü parolalar oluşturmak farkındalık çalışmaları sayesinde bilinçli kullanıcılar için sorun olmaktan çıkmış olmasına rağmen bu parolaların hatırlanması bir problem olarak varlığını devam ettirmektedir. Bu problemin çözümü için Bilişim Teknolojileri (BT) alanında çalışan kişilerin sıklıkla kullandıkları ama son kullanıcıların farkında olmadıkları parola cümlesi (passphrase) yöntemi kalıcı bir çözüm sağlayacaktır [20].

Tablo 2. İyi - Daha iyi - En iyi parola örnekleri.

İyi	Daha İyi	En İyi
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
Ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

Ayrıca, kurum ve şirketlerde parola güvenliğini sağlamak için parola oluşturma ve değiştirme politikaları oluşturulur. Bu politikalara göre hareket etmek tüm çalışanların yerine getirmesi gereken bir sorumluluktur.

Önerilen parola oluşturma yöntemleri

Dijital ortamlarda bulunan cihazları ve verileri yetkisiz erişimlere karşı korumak için klasik parolalar yerine, parola cümleleri kullanmak daha güvenilirdir [21]. Bir kullanıcı gizliliğe önem vermeye ve dijital güvenlik alışkanlıklarını geliştirmeye başladığında, atacağı ilk adımlardan biri parola cümlesi oluşturmak zorunda kalmasıdır. Parola cümlesi, kullanımda parolaya benzer ancak ek güvenlik için genellikle daha uzundur [10]. Parola cümlesi, klasik bir parola oluşturmaktan daha kolaydır, çünkü parola cümlesi bir kelimeden ziyade hatırlanması daha kolay bir cümle şeklindedir. Uzun parola cümleleri, sözlük ve kaba kuvvet saldırılarına karşı direnci artırır [22]. Ayrıca, parolanın belli zaman aralıklarında değiştirilmesi gerekiyorsa, bir parola cümlesinin hatırlanması daha kolay olabilir. Bu bağlamda; bu bölümde iyi bir parola cümlesi oluşturmak için yaklaşımlar sunulmaktadır.

Güçlü bir parola en az birer tane büyük harf, küçük harf, rakam ve özel karakter barındırmalıdır. Varyasyonu büyülttüğü için bu parolaların kriptografik olarak kırılması günümüz bilgisayarları ile neredeyse mümkün değildir. Bu parolaları oluşturup akılda tutmak bazen zor olabilmektedir. Bunun için bilişim sektöründe çalışanların sık kullandığı ancak son kullanıcıların pek bilmediği bir parola oluşturma yöntemi olan parola cümleleri kullanılmalıdır. Parola cümlesi ile parola oluşturmaya örnek olarak "Benim annem bir melektir." cümlesi kullanılacak olursa her ifadenin ilk iki karakteri alınır ise "Bean1me." parolası elde edilir. Parolanın anlamsız olması önemli değildir. Önemli olan parola cümlesinin unutulmamasıdır. Oluşturulacak parola paylaşılmamalı ve cümle unutulmamalıdır. Parola sözlük kelimesi olmamalıdır. Klasik yöntemler ile oluşturulan bir paroladan ziyade, bir parola cümlesi kullanmak daha güvenilirdir. İyi bir parola cümlesi oluşturmak için şunlara dikkat edilmelidir [22], [23].

- Kişi için anlamlı bir metin seçilmelidir.
- Parola cümlesi içerisinde (@ . - _ ~ ! # $ % ^ & *) özel karakterinden kullanılmalıdır.
- Parola cümlesinin uzun olması tercih sebebidir.
- Popüler bir şarkının sözleri gibi yaygın ifadeler kullanılmamalıdır.
- Karakterler, rakamlar, harfler birbirlerinin yerine kullanılmalıdır.
- En az 15, tercihen 20 karakterden oluşmalı ve tahmin edilmesi zor olmalıdır.
- Büyük harf, küçük harf, rakam ve tercihen en az bir noktalama karakteri içermelidir.

Hatırlanması kolay bir parola cümlesini oluşturmak için üç yöntemden biri tercih edilebilir:

İlk yöntemde kısa bir parola cümlesi tamamen küçük harfler ile oluşturulur. Bazı harfler büyük harfe çevrilir. Bazı harfler sayılara ve sembollere çevrilir. Bazı kelimeler kısaltılır veya farklı hecelenir. İlk yönteme şu iki örnek verilebilir:

Parola cümlesi: iki bardak buzlu su alalım
Değişimler: L-l→!, su→S, B-b→6, A-a→@, I-ı-İ-i→1
Kodlanmış Parola Cümlesi: 26@rd@k6uz!uS@!@!1m

Parola cümlesi: benim iki oğlum var
Değişimler: l→!, b→6, a→@, i→1, o→0, ğ→9, e→3, iki→2, var→V
Kodlanmış Parola Cümlesi: 63n1m209!umV

İkinci yöntem olarak birkaç kısa kelime belirlenir ve cümlenin ortasına kullanıcı için anlamlı olan bir sayı eklenir. Harfler için büyük harf ve sembol değişimleri yapılır. İkinci yönteme şu iki örnek verilebilir:

Parola cümlesi: Sinop 1876 Boyabat
Değişimler: S→&, i→1, o→(), a→@, t→7
Kodlanmış Parola Cümlesi: &1n()p1876B()y@b@7

Parola cümlesi: sağlam 2129 şifre
Değişimler: a→@, ğ→9, l→!, ş→$, i→1, e→3
İlk kelimenin ilk harfini büyük harfe çevir.
Kodlanmış Parola Cümlesi: S@9!@m2129$1fr3

Üçüncü yöntem olarak unutulmaz bir alıntı veya kelime öbeği seçilir. Bu öbekte özel karakter bulunmalıdır. Her kelimenin yalnızca ilk harfi kullanılır. Büyük harf

değişimi seçilecek kelime konumuna göre yapılır. Üçüncü yönteme şu iki örnek verilebilir:

Parola cümlesi: hiç çekmediğiniz şutların yüzde 100'ünü her zaman kaçıracaksınız.
Değişimler: Son kelimenin baş harfi büyük yazılacak.
Kodlanmış Parola Cümlesi: hçş%100hzK.

Parola cümlesi: ayda 1 yaşlıları ziyaret etmek için huzur evine gider misin?
Değişimler: İlk kelimenin baş harfi büyük yazılacak.
Kodlanmış Parola Cümlesi: A1yzeihegm?

Bazı kaynaklarda boşluk tuşunun parola oluşturulmasında kullanılabileceğinden bahsedilse de çoğu sistemde parola oluştururken buna izin verilmemektedir. Dolayısıyla @ . - _ ~ ! # $ % ^ & * () dışında özel karakter kullanılmamalıdır. Oluşturulan bu kodlanmış parola cümlelerinin ne kadar sürede kırılabileceği [24] referansında belirtilen çevrimiçi araç ile sınanabilir. Parola cümlesi oluşturmak ile ilgili son kullanıcılar kendilerine özel farklı yöntemler de geliştirebilirler. Bu çalışmada güçlü ve hatırlanması kolay parola oluşturulması amaçlandığı için belirtilen üç yöntemin kişisel siber güvenlik farkındalığı açısından katkı sağlayacağı değerlendirilmektedir.

Sonuç

Bilişim cihazlarına güvenli erişimi sağlamak önemlidir. Bununla beraber bu cihazlarda iletilen ve depolanan verilerin bütünlüğünü ve gizliliğini, son kullanıcıları bilinçlendirecek şekilde sağlamak da oldukça önemlidir. Çevrimiçi kişisel veriler siber saldırganlar için değerlidir. Çevrimiçi kimliğini, dijital verilerini, ağ ortamlarına bağlı cihazlarının siber güvenliğini sağlamak belli oranda son kullanıcının da sorumluluğundadır. Bu bağlamda; son kullanıcılar için çevrimiçi ortamlarda kişisel bilgilerin paylaşımında dikkat edilmesi gereken en önemli husus kişisel siber güvenlik açısından farkındalık sahibi olmaktır. Kişisel kimlik bilgileri ile kurum çalışanlarının kurumsal ve yönetimsel verilere erişilebilmesi durumu son kullanıcı farkındalığını daha da artırmaktadır. Kişisel verilerin korunmasına yardımcı olması için; "çevrimiçi olarak yapılması ve yapılmaması gerekenlerle ilgili bilgilendirmeler yapmak, son kullanıcı farkındalığı için önemlidir" ilkesi ile çevrimiçi verilerin güvenliğini artırmak amaçlanmıştır.

Kişisel verilerin ve cihazların siber güvenliğinin sağlanmasına odaklanılan çalışmada; son kullanıcılar tarafından bilinmeyen güçlü parola cümlesi oluşturma yöntemlerinden bahsedilmiştir. Geliştirilmiş parolalar oluşturmak, yüksek güvenlik gerektiren kurumlarda çalışanlar için bir zorunluluktur. Bu durum, kişisel siber güvenliğin artırılması açısından son kullanıcılar için de bir standart haline getirilebilir. Güvenli parola cümleleri yeni nesil parolalardır. Başka birinin tahmin etmesini zorlaştırmak için tek bir kelime yerine bir cümle kullanılır. Bu çalışmada ele alınan parola oluşturma yöntemlerinin uygulanabilir bir şekilde son kullanıcıya aktarılmasının kişisel siber güvenliğin oluşturulması açısından önemli bir farkındalık sağlayacağı değerlendirilmektedir.

Kaynakça

[1] N. Wiener, "Cybernetics or Control and Communication in the Animal and the Machine", MIT Press, 1961.

[2] M. Z. Gündüz ve R. Daş, "Nesnelerin İnterneti: Gelişimi, bileşenleri ve uygulama alanları", Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, c. 24, sy 2, 2018.

[3] M. Butavicius, vd., "When believing in technology leads to poor cyber security: Development of a trust in technical controls scale", Computers & Security, c. 98, 2020.

[4] M. Grobler, vd., "The importance of social identity on password formulations", Personal and Ubiquitous Computing, c. 25, sy 5, 2021.

[5] M. Z. Gündüz ve R. Daş, "Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri", Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 2016.

[6] M. Awad, vd., "Password security: Password behavior analysis at a small university", 5th International Conference on Electronic Devices, Systems and Applications, 2016.

[7] V. Taneski, M. Heričko, ve B. Brumen, "Password security - No change in 35 years?", 37th International Convention on Information and Communication Technology, Electronics and Microelectronics, 2014.

[8] M. Yıldırım ve I. Mackie, "Encouraging users to improve password security and memorability", International Journal of Information Security, c. 18, 2019.

[9] M. M. Algharibeh, G. Husari, S. Jaf, "A Data-Driven Password Strength Meter for Cybersecurity Assessment and Enhancement", 23rd Int Conf on High Performance Computing & Communications, 2021.

[10] P. A. Grassi, M. E. Garcia, ve J. L. Fenton, "Digital identity guidelines: revision 3", National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-63-3, 2017.

[11] https://www.kvkk.gov.tr/Icerik/2050/Kisisel-Veriler (erişim tarihi: 01.05.2022).

[12] Y. Guo, Z. Zhang, Y. Guo, ve X. Guo, "Nudging personalized password policies by understanding users' personality", Computers & Security, c. 94, 2020.

[13] F. Z. Glory, vd, "Strong Password Generation Based On User Inputs", IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference, 2019.

[14] T. Georg, B. Oliver, ve L. Gregory, "Issues of Implied Trust in Ethical Hacking", The ORBIT Journal, c. 2, 2018.

[15] Y. Ayrour, A. Raji, ve M. Nassar, "Modelling cyber-attacks: a survey study", Network Security, doi: 10.1016/S1353-4858(18)30025-4.
[16] B. Alhayani, vd., "Best ways computation intelligent of face cyber attacks", Materials Today: Proceedings, 2021, doi: 10.1016/j.matpr.2021.02.557.
[17] K. S. M. Moe ve T. Win, "Improved hashing and honey-based stronger password prevention against brute force attack", International Symposium on Electronics and Smart Devices, 2017.
[18] P. Maniriho, vd., "A study on malicious software behaviour analysis and detection techniques: Taxonomy, current trends and challenges", Future Generation Computer Systems, c.130, 2022.
[19] https://www.virustotal.com/gui/home/upload (erişim tarihi: 01.05.2022).
[20] Y. Zhao, vd., "Password Expiration Strategy: A Perspective of Ecological Memory", IEEE Fifth International Conference on Big Data Computing Service and Applications, 2019.
[21] B. Ur vd., "Design and Evaluation of a Data-Driven Password Meter", CHI Conference on Human Factors in Computing Systems, 2017.
[22] D. Pasquini, vd., "Reducing Bias in Modeling Real-world Password Strength via Deep Learning and Dynamic Dictionaries", USENIX Security Symposium, 2021.
[23] K. S. Walia, S. Shenoy, ve Y. Cheng, "An Empirical Analysis on the Usability and Security of Passwords", IEEE 21st International Conference on Information Reuse and Integration for Data Science, 2020.
[24] https://howsecureismypassword.net/ (erişim tarihi: 03.05.2022).